

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 USdistrictcourt.org@gmail.com (TARGET ACCOUNT),
 hosted at premises controlled by Google LLC, more fully
 described in Attachment A

Case No. MJ22-127

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, attached hereto and incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

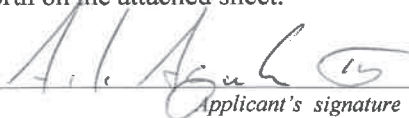
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 912	Impersonation of an Officer of the United States.

The application is based on these facts:

Please see Affidavit of Deputy U.S. Marshals Service Alberto Aguilar.

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Alberto Aguilar, Deputy U.S. Marshal

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/31/2022

City and state: Seattle, Washington



Judge's signature

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

INTRODUCTION AND AGENT BACKGROUND

2. This affidavit is submitted in support of an application to search **USdistrictcourt.org@gmail.com (TARGET ACCOUNT)**, which is hosted by Google LLC, a corporation based in Mountain View, California. The requested warrant would require Google to disclose law enforcement material listed in Section I of Attachment B and would authorize law enforcement officers to search for and seize the material listed in Section II of Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(Impersonation of an Officer of the United States) have been committed by an individual using the TARGET ACCOUNT. The requested material is expected to contain further evidence of fraud, as well as evidence that will help the government further establish and prove the identity of the person who is impersonating a United States Marshal. Therefore, probable cause exists to believe that the account will contain evidence and instrumentalities of 18 U.S.C. § 912.

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

STATEMENT OF PROBABLE CAUSE

6. On March 03, 2022, K.C., a pediatric health care provider at the Seattle Cancer Care Alliance and Seattle Children’s Hospital, emailed me an audio file of a voicemail from an individual who identified himself as United States Marshal Gary Hartnett. The voicemail stated that the individual had “important legal documents” to discuss with K.C. and requested that K.C. return his call at 206-350-9946.

7. When K.C. returned the call, the individual stated that the call was being conducted on a recorded line. The individual stated that she had failed to appear as an expert witness in a juvenile case on Monday, February 21, 2022, and now had two warrants out for her arrest. She was further informed by the individual that the United States Marshals had a

1 signed subpoena with her signature obtained by two uniformed officers on Wednesday,
2 January 19, 2022, at 2:07 P.M. The individual asserted that the subpoena had been delivered
3 to her at 825 Eastlake Avenue in Seattle, which is the address for the Seattle Cancer Care
4 Alliance clinic. To resolve this matter, she was instructed by the individual to proceed with
5 either the “criminal process” or “civil process.” For the “criminal process,” she could turn
6 herself in that day and be “apprehended” for up to 72 hours while bond and court dates are
7 reset, and this would be a part of her public record moving forward. Or, to proceed with
8 “civil process,” she would need to secure a civil surety bond with the court and appear at
9 court at 700 Stewart Street in Seattle on the same day to take a signature verification test to
10 prove that it was not her signature on the subpoena. Upon verification, the surety bond
11 payment would be refunded to her.

12 8. The individual provided the following warrant and bond information:
13 Contempt of Court (COC): 7-21-068 with bond of \$1,000 and Failure to Appear (FTA): 46-
14 64-025 with bond of \$1,000. The individual stated that K.C. could make the \$2000 payment
15 via digital payment systems Zelle or Google Pay to **TARGET ACCOUNT**. Digital
16 payment systems like Zelle and Google Pay allow users to send money to an account
17 identified by an email address (such as **TARGET ACCOUNT**) or a phone number.

18 9. K.C. stated that she questioned the validity of the individual’s statements
19 throughout the call. For example, she informed the individual that she could not have signed
20 the subpoena allegedly delivered to the clinic in January because she was not seeing patients
21 at the clinic in January. The individual responded that a secretary or security guard could
22 have signed for her and she was still legally responsible.

23 10. Additionally, although K.C. had returned the call at the number provided in the
24 voicemail (ending in -9946), the phone number that appeared on her caller ID screen was
25 206-370-8600. The individual instructed her to search the internet for the phone number, the
26 search engine associated the phone number with “US Marshals Service” in Seattle.

27 11. The individual insisted that he was a real United States Marshal, and she was
28 indeed in contempt of court for a juvenile case. He further said that there was a no-contact

1 order and gag-order placed by the judge, so if she tried to contact a lawyer or discussed this
2 matter with anyone else, she would forfeit the civil process and be prosecuted under the
3 criminal process that he had previously explained which would ultimately result in her arrest.
4 He also refused to provide any information about the case as it “involved a minor.”

5 12. While the individual had K.C. “on hold,” she called the United States District
6 Court in Seattle and spoke with court personnel who confirmed that the call was a scam.

7 **BACKGROUND REGARDING GOOGLE’S SERVICES**

8 13. In my training and experience, I have learned that Google provides a variety of
9 on-line services, including electronic mail (email) access, to the general public. Google
10 provides subscribers email and chat accounts at the domain name “@gmail.com.”

11 14. Subscribers obtain an account by registering with Google. When doing so,
12 Google asks the subscriber to provide certain personal identifying information. This
13 information can include the subscriber’s full name, physical address, telephone numbers and
14 other identifiers, alternative email addresses, and, for paying subscribers, means and source
15 of payment (including any credit or bank account number). In my training and experience,
16 such information may constitute evidence of the crimes under investigation because the
17 information can be used to identify the account’s user or users, and to help establish who has
18 dominion and control over the account.

19 15. Google typically retains certain transactional information about the creation
20 and use of each account on their systems. This information can include the date on which
21 the account was created, the length of service, records of log-in (i.e., session) times and
22 durations, the types of service utilized, the status of the account (including whether the
23 account is inactive or closed), the methods used to connect to the account, and other log files
24 that reflect usage of the account. In addition, email providers often have records of the IP
25 address used to register the account and the IP addresses associated with particular logins to
26 the account. As with subscriber records, IP address information can help to identify which
27 computers or other devices were used to access the email account, which in turn can be used
28

1 to identify the account's user or users, and to help establish who has dominion and control
2 over the account.

3 16. In some cases, email account users will communicate directly with an email
4 service provider about issues relating to the account, such as technical problems, billing
5 inquiries, or complaints from other users. Email providers typically retain records about
6 such communications, including records of contacts between the user and the provider's
7 support services, as well records of any actions taken by the provider or user as a result of
8 the communications. In my training and experience, such information may constitute
9 evidence of the crimes under investigation, because the information can be used to identify
10 the account's user or users.

11 17. In general, an email that is sent to a subscriber is stored in the subscriber's
12 "mail box" on the email provider's servers until the subscriber deletes the email. When the
13 subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to
14 the provider's servers, and then transmitted to its end destination. The email provider often
15 maintains a copy of received and sent emails. Unless the sender specifically deletes an email
16 from the email provider's server, the email can remain on the system indefinitely. Even if
17 the subscriber deletes the email, it may continue to be available on the email provider's
18 servers for some period of time.

19 18. A sent or received email typically includes the content of the message, source
20 and destination addresses, the date and time at which the email was sent, and the size and
21 length of the email. If an email user writes a draft message but does not send it, that message
22 may also be saved by the email provider but may not include all of these categories of data.

23 19. In addition to email and chat, Google offers subscribers numerous other
24 services including, (i) Location History, which saves information about the physical
25 locations of devices logged into a Google account; and (ii) Web & Activity, which saves
26 information about Google web searches and browsing activity conducted by a user logged
27 into a particular Google account.
28

1 20. Information stored in connection with an email account may provide crucial
2 evidence of the “who, what, why, when, where, and how” of the criminal conduct under
3 investigation, thus enabling the United States to establish and prove each element or
4 alternatively, to exclude the innocent from further suspicion. In my training and experience,
5 the information stored in connection with an email account can indicate who has used or
6 controlled the account. This “user attribution” evidence is analogous to the search for
7 “indicia of occupancy” while executing a search warrant at a residence. For example, email
8 communications, contacts lists, and images sent (and the data associated with the foregoing,
9 such as date and time) may indicate who used or controlled the account at a relevant time.

10 21. Information maintained by the email provider can show how and when the
11 account was accessed or used. For example, email providers typically log the IP addresses
12 from which users access the email account, along with the time and date of that access. By
13 determining the physical location associated with the logged IP addresses, investigators can
14 understand the chronological and geographic context of the email account access and use
15 relating to the crime under investigation. This geographic and timeline information may tend
16 to either inculcate or exculpate the account owner. Additionally, information stored at the
17 user’s account may further indicate the geographic location of the account user at a particular
18 time (e.g., location information integrated into an image or video sent via email).

19 22. Based on my training and experience, I know that criminals sometimes use
20 multiple email accounts. These accounts may be linked together in that they may share
21 common recovery information (for example, the same recovery phone number or email
22 address), or Google records may show that the accounts were accessed by the same device or
23 IP address. Identifying linked accounts can assist investigators in determining the true
24 identities of the persons using the accounts. Accordingly, the requested warrant would
25 require Google to provide subscriber and other non-content information associated with
26 accounts linked to the **TARGET ACCOUNT**.

27 23. This Application seeks a warrant to search all responsive records and
28 information under the control of Google, a provider subject to the jurisdiction of this court,

1 regardless of where Google has chosen to store such information. The government intends
2 to require the disclosure pursuant to the requested warrant of the contents of wire or
3 electronic communications and any records or other information pertaining to the customers
4 or subscribers if such communication, record, or other information is within Google's
5 possession, custody, or control, regardless of whether such communication, record, or other
6 information is stored, held, or maintained outside the United States.

7 24. This warrant will be executed under the Electronic Communications Privacy
8 Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the
9 warrant to require Google to disclose to the government copies of the records and other
10 information (including the content of communications and stored data) particularly described
11 in Section I of Attachment B. Upon receipt of the information described in Section I of
12 Attachment B, government-authorized persons will review that information to locate the
13 items described in Section II of Attachment B.

14 **REQUEST FOR NONDISCLOSURE AND SEALING**

15 25. The government requests, pursuant to the preclusion of notice provisions of
16 Title 18, United States Code, Section 2705(b), that Google be ordered not to notify any
17 person (including the subscriber or customer to which the materials relate) of the existence of
18 these warrants for such period as the Court deems appropriate. In this case, such an order is
19 appropriate because the search warrants relate to an ongoing criminal investigation and
20 disclosure would provide the targets with information about the government's investigation
21 that could be used to frustrate further investigative efforts.

22 26. I further request that the Court order that all papers in support of this
23 application, including the affidavit and search warrant, be sealed until further order of the
24 Court. These documents discuss an ongoing criminal investigation that is neither public nor
25 known to all of the targets of the investigation. There is good cause to seal these documents
26 because their premature disclosure may give the subjects an opportunity to flee from
27 prosecution, dissipate assets, destroy or tamper with evidence, change patterns of behavior,
28 notify confederates, or otherwise seriously jeopardize the investigation.

28. Based on the foregoing, I believe there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States Code, Section 912 (Impersonation of an Officer of the United States) will be found in the **TARGET ACCOUNT**, as more fully described in Attachment A to this Affidavit. I therefore request that the Court issue a warrant authorizing a search of the **TARGET ACCOUNT**, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

29. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone on 31st day of March, 2022.

State Vaughan
S. KATE VAUGHAN
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to the electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following account: **USdistrictcourt.org@gmail.com (TARGET ACCOUNT)**, as well as all other subscriber and log records associated with TARGET ACCOUNT, which is located at premises owned, maintained, controlled or operated by Google LLC, an email and service provider that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B**Particular Things to be Seized****I. Information to be disclosed by Google LLC (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the **TARGET ACCOUNT** identified in Attachment A:

- a. The contents of all emails associated with the **TARGET ACCOUNT**, including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each emails, the date and time at which each email was sent, and the size and length of each email;
- b. All subscriber records associated with the specified accounts, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;
- c. All records or other information stored by any individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

- d. any Google Chat/Messenger information and/or records, including any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on servers;
- e. any Google Search Console content from inception to the present;
- f. any Google Web & Activity content from inception to the present;
- g. any Google Chrome Sync content from inception to the present;
- h. any Google Location History content from inception to the present;
- i. any account history, including any records of communications between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service;
- j. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

This Search Warrant also requires Google to produce the following information for **TARGET ACCOUNT**:

- a. list of all other accounts linked to the TARGET ACCOUNT because of cookie overlap;
- b. a list of all other accounts that list the same SMS phone number as the TARGET ACCOUNT;
- c. a list of all other accounts that list the same recovery email address as the TARGET ACCOUNT;

- 1 d. a list of all other accounts that shared the same creation IP address as the
2 TARGET ACCOUNT within 30 days of creation;
- 3 e. The Accounts referred to in subparagraphs (a) through (d) above are
4 referred to herein as the “Linked Subject Accounts.” Google shall produce
5 subscriber records for each of the Linked Subject Accounts including 1)
6 names, email addresses, and screen names; 2) physical addresses; 3)
7 records of session times and durations; 4) length of service (including start
8 date) and types of services utilized; 5) telephone or instrument number or
9 other subscriber number or identity, including any temporarily assigned
10 network address such as internet protocol address, media access card
11 addresses, or any other unique device identifiers recorded by Google in
12 relation to the account; 6) account log files (login IP address, account
13 activation IP address, and IP address history); 7) detailed billing
14 records/logs; 8) means and source of payment; and 9) lists of all related
15 accounts.
- 16 f. All records and other information (not including the contents of
17 communications) relating to the Linked Subject Accounts, including:
- 18 i. Records of user activity for each connection made to or from the
19 Linked Subject Accounts from January 1, 2021 to the present,
20 including log files; messaging logs; the date time, length, and
21 method of connections, data transfer volume; user names; and source
22 and destination Internet Protocol Addresses; cookie IDs; browser
23 type;
- 24 ii. Information about each communication sent or received by the
25 Linked Subject Accounts from January 1, 2021 to the present,
26 including the date and time of the communication, the method of
27 communication, and the source and destination of the
28 communication (such as source and destination email addresses, IP
addresses, and telephone numbers); and

- 1 iii. All records pertaining to devices associated with the accounts to
2 include serial numbers, model type/number, IMEI, phone numbers,
3 MAC Addresses.

4 **The Provider is hereby ordered to disclose the above information to the**
5 **government within 14 days of service of this warrant.**

6 **II. Information to be seized by the government**

7
8 Upon receipt of the information described in Section I, the government shall
9 review the production and may seize the following material:

10 The following information that constitutes evidence and instrumentalities of
11 violations of Title 18 United States Code, Section 912 (Impersonation of an Officer of the
12 United States) for the **TARGET ACCOUNT**:

- 13 a. Material containing personal identifying information or account access
14 information of any person.
- 15 b. Material that serves to identify any person who uses or accesses or who
16 exercises in any way any dominion or control over the TARGET
17 ACCOUNTS;
- 18 c. Material evidencing the times and methods by which the TARGET
19 ACCOUNTS was accessed;
- 20 d. Material that serves to identify any persons connected to any person who
21 accesses or who exercises in any way any dominion or control over the
22 TARGET ACCOUNTS; and
- 23 e. Material evidencing the user's state of mind as it relates to the crimes under
24 investigation;
- 25 f. Material that serves to identify any other accounts related to the TARGET
26 ACCOUNTS; including accounts that share common recovery information
27 or that are linked by cookies or in any other way;
- 28

- 1 h. Content that may identify any alias names, online user names, “handles”
2 and/or “nics” of those who exercise in any way any dominion or control
3 over the accounts as well as records or information that may reveal the true
4 identities of these individuals;
- 5 i. Log records, including IP address captures, associated with the account;
- 6 j. Subscriber records associated with the accounts, including 1) names, email
7 addresses, and screen names; 2) physical addresses; 3) records of session
8 times and durations; 4) length of service (including start date) and types of
9 services utilized; 5) telephone or instrument number or other subscriber
10 number or identity, Including any temporarily assigned network address
11 such as internet protocol address, media access card addresses, or any other
12 unique device identifiers recorded by Google in relation to the account; 6)
13 account log files (login IP address, account activation IP addresses, and IP
14 address history); 7) detailed billing records/logs; 8) means and source of
15 payment; and 9) lists of all related accounts;
- 16 k. Records of communications between Google and any person purporting to
17 be the account holder about issues relating to the account, such as technical
18 problems, billing inquiries, or complaints from other users about the
19 specified account. This to include records of contacts between the
20 subscriber and the provider’s support services, as well as records of any
21 actions taken by the provider or subscriber as a result of the
22 communications;
- 23 l. Android or Apple identification number, MEID, and cellular telephone
24 number; and
- 25 m. Information identifying accounts that are linked or associated with the
26 account.
27
28

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature